VA Software Assurance

Office of Information Security

Secure Coding Tips

Tip: Encapsulation Coding Errors Can Lead To Vulnerabilities

This week's Secure Coding Tip is about encapsulation coding errors[1] can introduce vulnerabilities into VA applications. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [2] , and enforced as part of the ATO issuance process.[3]

This type of vulnerability has to do with coding errors related to sufficiently encapsulating critical data or functionality. An example is mixing trusted and untrusted data in the same data structure or structured message.[4] Security feature coding errors such as these are errors that the HP Fortify Static Code Analyzer (SCA) can detect.

Read more...

[1] MITRE Common Weakness Enumeration (CWE) **CWE-485: Insufficient Encapsulation**
[2] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.
[3] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.
[4] MITRE Common Weakness Enumeration (CWE) **CWE-501: Trust Boundary Violation**

More Information

For more information about the VA Software Assurance Program Office, please visit our website here.

Resources

VA Software Assurance Support Site

VA Code Review Standard Operating Procedures

VA-Licensed Fortify Request Instructions

VA Software Assurance Frequently Asked Questions

Training

VA Code Review Process

VA Fortify End User Course

VA Secure Coding Course